Краснознаменский городской колледж. Корпус Селятино.

**"Политика безопасности компьютерного класса"**

Выполнил студент группы ОИСПс-122

Талызин Никита Владимирович

Селятино 2024

**Политика безопасности**

**Что такое Политика безопасности.**

Политика безопасности – это набор правил, определяющих методы, степень защиты прикладной системы и регламентирующих прав доступа к объектам системы. Политика безопасности содержит параметры, имеющие глобальное воздействие на степень защиты системы. Определение степени защиты для отдельных объектов производится с помощью методов разграничения доступа.

**Где применяется.**

Политика безопасности применяется для обеспечения защиты информационных систем, сетей и данных от различных угроз, таких как несанкционированный доступ, взлом, утечка данных и другие киберугрозы.

Она определяет основные направления деятельности организации в области информационной безопасности, устанавливает ответственность и порядок действий в случае инцидентов безопасности.

Политика информационной безопасности решает следующие задачи:

Защита конфиденциальной информации компании от несанкционированного доступа, изменения или уничтожения.

Обеспечение непрерывности работы информационных систем и сервисов компании, даже в случае кибератаки или других инцидентов.

Соответствие требованиям законодательства в области информационной безопасности и защиты персональных данных.

Снижение риска финансовых потерь компании из-за нарушения информационной безопасности.

Улучшение имиджа компании как надёжного партнёра, заботящегося о безопасности данных своих клиентов и партнеров.

**Цели и задачи.**

Основной целью является обеспечение информационной безопасности Учреждения, что предполагает эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности, подчиненное единому замыслу.

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация рисков ИБ.

**Правила компьютерного класса.**

1. Не оставлять компьютер включенным без присмотра
2. Не пить и не есть за компьютером
3. Не открывать окно
4. Не скачивать посторонние программы на компьютер
5. Все файлы сохранять строго на флэшку
6. Удалять за собой ненужные файлы
7. Выходить из своих аккаунтов соц. Сетей, программ, приложений

**Правила работы за компьютером**

1. Не скачивать программы с посторонних сайтов. Скачивать только с официальных источников (Microsoft Store).
2. Не оставлять пароли от аккаунтов на компьютере.
3. Выходить из аккаунтов соц. Сетей, программ и т.д.
4. Сохранять нужные файлы на флэшку.
5. Удалять ненужные файлы.
6. После завершения работы, закрывать все программы и приложения.

**Что делать, если с ПК что-то не так.**

1. Сообщить о проблеме преподавателю или главному по компьютеру.
2. Если преподаватель или главный сможет устранить ошибку, то вы можете продолжать работу.
3. При повторной ошибке или новой ошибке, поменяйте ПК, перед этим не забудьте сообщить об ошибке преподавателю.